password is the password, and denying access if said general access password is not the password.

REMARKS

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached Appendix is captioned "**Version with Markings to Show Changes Made.**"

As a preliminary matter, Applicants appreciate the Examiner's time and the courtesy extended during the January 29, 2003, telephonic interview with Applicants' representatives. As discussed during the interview, Applicants amended claims 1 and 18 to clarify that the storing apparatus is for use with a computer-based system, as suggested by the Examiner.

As a further preliminary matter, Applicants again request acknowledgement of the references cited in a Supplemental Information Disclosure Statement received on August 15, 2000. A copy of a PTO Form 1449 listing those references is enclosed.

Claims 1-21 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicants respectfully traverse the Examiner's §101 rejection. As explained during the telephone interview and acknowledged by the Examiner, because with the use of the default password and the access password (i.e., the write/read password 62 or the read only password 64), an authorized first user can selectively permit a second user to

access the information without the password. Please note that for clarity, the access password refers to both the user of the write/read password and/or the read only password 64. In addition to the access password, a default password is kept in the password preserving unit as a continuous authentication of authorized or nonauthorized access to the medium. In other words, the access password remains the same while the first user changes the default password for permitted access by the second user. The present invention solves, among other things, the problem of always changing the password of the first user in order to allow usage by the second user without the password. Thus, Applicants submit that the present invention is useful, and is directed to a statutory subject matter. Accordingly, Applicants respectfully request that the §101 rejection of claims 1-21 be withdrawn.

Claims 1-21 stand rejected under 35 U.S.C. §112, first paragraph. Applicants respectfully traverse because the term "general access password" can better represent the multiple passwords that are stored in the password preserving unit, as recited in the claims. As described in one embodiment of the present invention, a password preserving area 45 stores multiple passwords, specifically a default input password 60, a write/read password 62, and a read only password 64, for access to the hard disk drive 44 (FIG. 2; Applicants' specification, page 16, lines 8-11). Again, for clarity, an access password will be used to refer to both the write/read password 62 and/or the read only password 64. For an authorized access to the drive 44, the default input password and the access password stored in the password preserving area 45, must match (Applicants' specification, page 17, lines 20-25). Since the labeling of these passwords can be changed, Applicants believe that the term

"general access password" would better reflect the multiple passwords stored in the password preserving area 45 and used to determine authorized usage to the drive 44. More specifically, according to the language of claims 1 and 8, two passwords (i.e., a password and a general access password) are stored and used by the storing apparatus. Accordingly, for these reasons, Applicants respectfully request that the §112 rejection of claims 1-21 be withdrawn.

Claims 1-2, 5 and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rupp Corporation and/or Hideo. Applicants respectfully traverse because the cited references do not disclose or suggest a storing apparatus for use with a computer-based system that includes a password preserving unit for preserving a general access password and a password; and a password verifying unit for allowing access if the password is entered, and if the password is not entered, comparing the general access password with the password, allowing access if the general access password is the password, and denying access if the general access password is not the password, as recited in claim 1. Applicants further traverse because the cited references do not disclose or suggest a method of protecting access to information recorded on a medium with a password for use with a computer-based system that includes a password preserving step and a password verifying step, as recited in claim 18.

As previously indicated, Applicants amended claims 1 and 18 to clarify that the storing apparatus is for use with a computer-based system, as suggested by the Examiner. It is Applicants' understanding that none of the cited references disclose the features of a

password and a general access password, as claimed, which was acknowledged by the Examiner during the telephone interview.

In particular, as discussed in the interview with the Examiner, two separate passwords are needed to control access to the medium, specifically in one embodiment, the default input password/user input password and the access password. The default input password is used for authenticating authorized access to the medium, the access password is used for defining access rights to the medium, and the user input password is a password entered by a user. In one embodiment, the access password is divided into a write/read password 62 and a read only password 64, which defines the authorized access rights to the medium as indicated (Applicants' specification, page 16, lines 8-27).

As a result, unlike the cited references, the present invention does not use a particular default password to lock the hard drive (i.e., the Rupp reference) or an IC card to match a password stored in the memory (i.e., the Hideo reference). Rather, in the present invention, when an authorized usage is initiated by the default input password (i.e., stored in memory) or a user input password (i.e., entered by a first user) matching the access password, a second user can then access the medium continuously (Applicants' specification, page 5, lines 18-24). Once the second user finishes the work, the default input password is changed in order to end the authorized usage of the medium (Applicants' specification, page 43, lines 21-24). However, note that only the default input password is changed, and the access password is not changed. As a result, the first user can temporarily authorize usage of the medium without changing the access password that is known only to the first user.

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Claims 1 and 18 as follows:

1. (Twice Amended) A storing apparatus for use with a computer-based system in which a first user can protect access to information recorded on a medium with a password, and can selectively permit said first user and a second user to access the information without the password, comprising:

a password preserving unit for preserving a general access password and the password; and

a password verifying unit for allowing access if the password is entered, and if the password is not entered, comparing the general access password with the password, allowing access if the general access password is the password, and denying access if the general access password is not the password.

18. (Amended) A ~~storing~~ method of protecting access to information recorded on a medium with a password for use with a computer-based system~~from an access by a password~~, comprising:

a password preserving step of preserving ~~a default input password and a password for access protection~~the password and a general access password; and

a password verifying step of controlling the access protection by comparing a user input password input by a user with the password when there is the user input password, allowing access if the user input password is the password, and denying access if the user input password is not the password, and for controlling access protection by comparing said general access password substituted for said user input password with the password when there is no user input password, allowing access if said general access password is the password, and denying access if said general access password is not the password~~substituting said default input password for a user input password and comparison collating with said password for access protection when there is no password input from the user and for controlling the access protection by comparison collating said user input password with said password for access protection when there is the password input from the user~~.

In the Rupp reference, the master password and the default password do not correspond to the access password and the default input password, as recited in the claims. The master password disclosed in the cited reference allows a user to have full access to all hard drives with a single master key without regard to any individual passwords. The function of the master password is well established in the art. On the other hand, the function of the default password, as disclosed in the Rupp reference, allows a user to set a password once, and the system will automatically lock the hard drive using the default password. Thus, users can initiate a lock with a single key stroke without entering any password by the user.

The default password is nothing more than a typical user password assigned to an individual user, which is again well established in the art. The novel feature of Rupp is that the system is configured to automatically use the default password to lock the hard drive. Thus, as shown, the master password and the default password do not correspond to the access password and the default input password, as recited in the claims. In fact, the invention disclosed in the Rupp reference relates to different benefits and purposes from the present invention.

The Hideo reference discloses nothing more than an IC card system with a list of stored passwords that correspond to a plurality of cards. In particular, an identification data X is stored on the IC card and when inserted, the system extracts a password corresponding to the data X stored in the memory of the device. The same password is then stored on the card. Contrary to the Examiner's assertion, the same exact password is stored on the device and the IC card.

In contrast, the default input password and the access password are two separate and independent passwords stored in the password preserving area 45. Thus, it cannot be said that the single password that is stored on the device and the IC card in Hideo corresponds to the password and the general access password, as recited in the claims. Moreover, the invention disclosed in the Hideo reference also has different benefits and purposes from the present invention. Consequently, there is no suggestion or motivation from either the Rupp reference or the Hideo reference to use a password and a general access password, as recited in the claims. Accordingly, Applicants respectfully request that the §103 rejection of claims 1 and 18 be withdrawn.

Since claims 2-17 and 19-21 depend upon either claim 1 or claim 18, respectively, they necessarily include all of the features of the independent claims plus other additional features. Thus, Applicants submit that the §103 rejection of claims 2-17 and 19-21 has also been overcome for the same reasons mentioned above to overcome the §103 rejection of independent claims 1 and 18. Applicants respectfully request that the §103 rejection of claims 2-17 and 19-21 be similarly withdrawn.

For all of the above reasons, Applicants respectfully request reconsideration and allowance of all pending claims. The Examiner should contact the undersigned attorney if an interview would expedite prosecution.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By 

Patrick G. Burns
Registration No. 29,367

February 6, 2003

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315
K:\1990\62597\Amend B.doc

Form PTO-1449 (Rev. 8-88) U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.1990.62597	Serial No. 09/159,833
INFORMATION DISCLOSURE CITATION (Use several sheets if necessary)	Applicant: Utsumi et al.	
	Filing Date: 9-24-98	Group: 2131

U.S. PATENT DOCUMENTS

Examiner Initial*		Document Number	Date	Name	Class	Subclass	Filing Date If Appropriate
		5,533,125	July 2, 1996	Bensimon et al.	380	4	July 18, 1995

FOREIGN PATENT DOCUMENTS

		Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
		770 997	May 2, 1997	Europe			X	
		95/14265	May 26, 1995	WIPO			X	
		3 262 067	Nov. 21, 1991	Japan			Abs.	

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner	Date Considered

*Examiner: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.